Shaul Shay *and* ***Esther Shay***
Institute for National and International Security
Email: sc.shaulshay@gmail.com

DOI
Original Research Paper
Received: May 21
Accepted: June 25

THE MEDICAL INTELLIGENCE AND THE BIOTERRORISM

Abstract: *The definition of bioterrorism: "Bioterrorism refers to the intentional release of biological agents or toxins for the purpose of harming or killing humans, animals or plants with the intent to intimidate or coerce a government or civilian population to further political or social objectives."*[i] *The threat from bioterrorism is real, with current reports indicating that individuals, terrorist groups and criminals have both the capability and intention to use biological agents to cause harm to society. The damage caused by such an event could reach untold magnitude, causing widespread illness and death, and instilling fear and panic on a global scale. The spread of an infectious or toxic biological agent can happen without warning, while the response to a biological event, whether naturally occurring, accidental or deliberate, relies on coordination across multiple sectors. Medical intelligence (MEDINT) is a critical component in dealing with the threat of biological terrorism. The Covid-19 crisis has imposed the need for medical intelligence to adapt to the new security reality and it is clear evidence of the crucial importance of medical intelligence for prevention and minimization of the serious consequences that epidemics may have on public health and national security on all its components. Medical intelligence related to the threat of public health emergencies, including terrorism. Intelligence implies the application of the intelligence cycle in the field of medicine. It implies the collection and processing of data, assessment of data and predictions of the risks. It involves information applied to the identification, characterization, and management of a risk, as applied to both medical and nonmedical countermeasures. The article will review the threat of biological terrorism and the contribution of medical intelligence to deal with this threat.*

Key words: *bioterrorism, biosecurity, medical intelligence (MEDINT), intelligence cycle.*

Introduction

The COVID-19 pandemic has reignited debates and discussions around healthcare systems' biosecurity vulnerabilities and cast a spotlight on the potential weaponization of biological agents. The COVID-19 crisis has imposed the need for medical intelligence (MEDINT) to adapt to the new security reality. With the extraordinary disruption brought about by COVID-19, terrorist groups and other malicious actors may understand the catastrophic damage that can be caused by highly transmissible pathogens and other biological agents, and to use them to deliberately cause the next pandemic.[ii] Before we can really understand the role of intelligence in understanding and managing bio-threats, it is critical first to step back and assess the biosecurity environment and the threat of bioterrorism. The security environment can be defined as the sum of threats and risks that any intelligence capability must understand as fully as possible if it is to reduce uncertainty and provide warning to decision-makers. Depending on the context, the security environment can be made up of a multitudinous and diverse number of threats and risks. [iii] State based biological weapons programs, particularly those developed by Cold War protagonists—the former USSR and USA from 1945 until 1970s (for the USA), and up to the 1990s for the Soviet Union, dominated policy maker's understanding and framing of the bio-threat environment. [iv] These were large, industrial programs that produced vast quantities of dangerous pathogens, such as highly virulent anthrax, plague and tularemia.

After the end of the Cold War, biological weapons lost the status of offensive weapons of mass destruction. Concern, however, was also raised that other less stable or rogue states (Iraq, Iran, Syria and North Korea) were seeking to develop biological weapons.[v] The biosecurity threat environment after the Cold War shifted away from an almost exclusive array of potential state-based threats (state sponsored biological weapons programs) to an increasing number of non-state actors —primarily terrorists.[vi]

The threat of bioterrorism

Biological terror (bioterror) is the deliberate use of biological weapons to directly harm human beings. The extent of injury depends on the agent used, its biological characteristics, and means of dissemination. Such harm can also be indirect, aimed at creating panic, demoralization,

damage to national image, and political and economic damage. There are several definitions of bioterrorism:

Bioterrorism is the use of biological weapons to cause death, fear, economic disruption and/or political upheaval in order to achieve political, ideological, social and/or religious goals.[vii] The INTERPOL's definition of bioterrorism: "Bioterrorism refers to the intentional release of biological agents or toxins for the purpose of harming or killing humans, animals or plants with the intent to intimidate or coerce a government or civilian population to further political or social objectives".[viii]

While the Biological Weapons Convention established in 1975 prohibits the development, production, acquisition, transfer, stockpiling and use of biological and toxin weapons by the 183 states (as of September 2021) that have ratified and acceded the treaty, little can stop rogue actors or terrorist organizations from harnessing existing or creating novel biothreats using the technology available today.[ix]

The principal biological threat today comes from terror groups, since a biological attack requires only small amounts of material that can be concealed easily and dispersed secretly. In addition to creating huge casualties and potent psychological effect, biological weapons also could create extensive peripheral and indirect economic, social, and political damage.

Biological attacks can be:

- Overt attack, which can be detected by an explosion, smoke or other obvious signs.
- Covert attacks, which involve quiet or camouflaged dissemination by unseen aerosols, individual infections, or the poisoning of food or water sources.

The type of attacks has immediate implications for its effect and the possibility of taking appropriate defensive action. An overt attack triggers immediate suspicion and subsequent identification of the biological agent. Pre planed preventive actions can then be taken.

In contrast, a covert attack, in the absence of concrete intelligence information, may be discovered only after the first wave of casualties appears. This could be several hours or days after the attack itself, depending on the agent.

The preferred targets for biological attack are generally crowded places such as shopping centers, train stations (especially underground stations), airport terminals, sports stadiums, halls and large dining areas.

To prevent biological weapons and / or their components from reaching terrorists organizations, we must first identify their sources and the channels through which the terrorist might obtain them. In the current circumstances several such channels can be posited:

- A terror supporting state could actively and directly supply biological armaments or components from its own arsenal to a terror organization it supports. For example, Iran, in the framework of its general strategy, could supply bioweapons to terror organizations of the "axis of resistance" such as Hezbollah, the Houthi rebels or Iraqi Shia militias.
- Terror organizations could steal biological weapons, components or information from countries with biological arsenals or weapon programs. [x]
- Terrorist groups could produce bioweapons on their own. Biological agents, methods and research results of interest to terrorist groups can reach them from civilian research laboratories in academia, medical centers and industry. In a few cases, proofs have been found of intentions, programs and actual attempts to do so, including the construction of a laboratory infrastructure appropriate for bioweapons production.
- Terrorists can use dual use research and technology to develop bio weapons. Dual use research and technology means activities, knowledge and equipment, which is used for legitimate research (for example the development of vaccines) but could also be used inappropriately by those motivated by politics or crime.[xi]
- Another threat is the "lone wolf" bioterrorist - a highly skilled and trained individual could use its knowledge to create biological agents under the guise of legitimate research for illegitimate ends.

There are several terror events that made political leaders to shift their focus on bio-threat actors away from states to groups and even individuals and why ‘bio-terrorism’ became the policy priority .

The first event occurred in 1995 when the Japanese doomsday cult Aum Shinrikyo released sarin nerve gas into the Tokyo subway system killing 12 people and injuring 5000 more .

Investigations later revealed that the cult had also acquired anthrax and botulinum toxin and was attempting to weaponize it against various Japanese government political, military and public institutions. The cult failed to cultivate sufficiently lethal strains of botulinum toxin and anthrax and its plans were foiled also by other technical challenges.

The second event which elevated the importance of bio-terrorism for policy-makers was discoveries by US forces post the 2001 invasion of Afghanistan of technical documents and equipment in a biological weapons laboratory under construction near Kandahar. Additional documents were also found in a close by al Qaeda training camp—detailing the terrorists groups plans to develop a biological weapons capability. The documents and searches of the laboratory showed that the al Qaeda program was in its early stages and the group had not yet obtained operational capabilities.

In his memoirs, former Director of the CIA, George Tenet mentioned two individuals (Rauf Ahmad and Yazid Sufaat), who were recruited by Bin Laden's deputy, Ayman al-Zawahiri, to develop this capability. After the US led invasion of Iraq, coalition forces reported that Ansar al-Islam, an Al Qaeda affiliate group, was engaged in the production of ricin, but there was no evidence that it reached a stage of large scale weaponization that could cause mass casualties.

The third bio-terror event involved the 2001 release of anthrax spores in the US mail system. In September and October 2001, seven envelopes containing a dried powder form of anthrax spores were posted to several media outlets and to the US Senate offices of Senators Thomas Daschle and Patrick Leahy.

The investigation resulted in the US Department of Justice determining that a single spore batch created by anthrax specialist Dr. Bruce E. Ivins at the US Army Medical Research Institute of Infectious Diseases (USAMRID) was the parent material for the letter spores. In July 2008, Ivins committed suicide before being indicted .

The fact that the 'attacker' had been a scientist with access to highly controlled dangerous biological agents focused intelligence agencies on the threats and risks associated with dual-use research and technology.

The threat of Bioterrorism becomes increasingly pressing as rapid, globally distributed technology advances continue to lower the barriers to the synthesis and engineering of pathogens and other biological agents, thereby enabling a wider range of actors to engage in this type of work—including non-state actors.

The threat from bioterrorism is real, with current reports indicating that individuals, terrorist groups and criminals have both the capability and intention to use biological agents to cause harm to society. As Lawrence Kerr noted, "at one point in time, there were 3,000 named apocalyptic groups around the world, including terrorists solely interested in annihilation of

humans." [xii] The strategy for combating biological risks posed by non-state actors is different than the approach that is likely to be most effective for preventing development and use of bioweapons by states. One key reason for this is that it is very difficult to shape intent of non-state actors and to deter them from pursuing bioweapons development or use.[xiii]

This is because many non-state actor groups are not motivated by the same rational political, military, and economic goals that motivate most states. As a result, it is unlikely that those responsible for guarding against bioterrorism threats could ever get to a point of high confidence that there are no groups anywhere around the world with the intention of causing large-scale catastrophic damage and who would use biology to do so given the opportunity.[xiv]

We have to assume that such groups exist now and that they will continue to exist for the foreseeable future. In fact, there is publicly available evidence that such groups have existed in the not-distant past. We should assume that there are other extremist groups in existence at the moment with similar intentions.[xv]

A study aims to provide an epidemiological description of all terrorism-related attacks using biological agents sustained between 1970 and 2019, say that 33 terrorist attacks involving biological agents were recorded between 1970 and 2019, registering 9 deaths and 806 injuries. 21 events occurred in the United States, 3 in Kenya, 2 each in both the United Kingdom and Pakistan and a single event in Japan, Columbia, Israel, Russia and Tunisia.[xvi] Data collection was performed using a retrospective database search through the Global Terrorism Database (GTD).

Twenty of the attacks involved anthrax, 5 involved salmonella, 3 involved ricin, 2 involved faucal matter, 1 involved botulinum toxin, 1 involved the use of HIV infected razor blades and 1 involved either ricin or anthrax. Seven of the recorded deaths were linked to anthrax attacks and 2 remaining deaths were related to salmonella incidents. Of the 806 injuries reported, 776 were related to 2 attacks involving salmonella, 25 were related to anthrax events and 1 was related to an event involving faecal matter as a biological agent. Anthrax has been the most commonly used in previous bioterrorism events with the vast majority of reported attacks occurring in the United States by a single suspected perpetrator.

The reported use of biological agents as a terrorist weapon is extremely rare and certainly not enough to make analytical generalizations. Despite its apparent rarity, however, bioterrorism has the ability to inflict mass injuries unmatched by conventional weapons. A comprehensive

strategy for preventing such groups from using biology to cause catastrophic harm on a global scale will require investment of significantly more resources in biothreat intelligence and law enforcement capabilities.

The medical intelligence (MEDINT)

Intelligence is the discipline that carries out the planning, collection, analysis and generation of products for the decision-makers of a country, sector or organization. Intelligence refers to specific information that has been collected in order to answer context-driven requirements and has been analyzed and assessed to answer these requirements. This practice is typically driven by the intelligence cycle, which describes an ongoing and circular sequence. [xvii]

Previously, Intelligence was related more to security activities of all kinds, but currently, because it is an adequate process of obtaining analysis, and generation of products for decision making, its use has spread to various areas such as the financial, economic, health sector, etc. Medical intelligence represents a critical intelligence capability to monitor and evaluate risks to health within frameworks that either prioritize military considerations or form a significant component of national security interests.

This paper presents medical intelligence (MEDINT) as a specific discipline of intelligence work. Medical intelligence related to the threat of public health emergencies, including terrorism and medical intelligence is critically important for early detection of groups looking to carry out a bioweapons attack, so they can be apprehended before they make an attempt.

The United States Department of Defense uses the following definition of medical intelligence: "That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. Also called MEDINT." [xviii]

NATO defines MEDINT as: "Medical intelligence is the product resulting from the directed collection and assessment (processing) of medical, bio-scientific, epidemiological, environmental and other information related to human or animal health, to identify threats

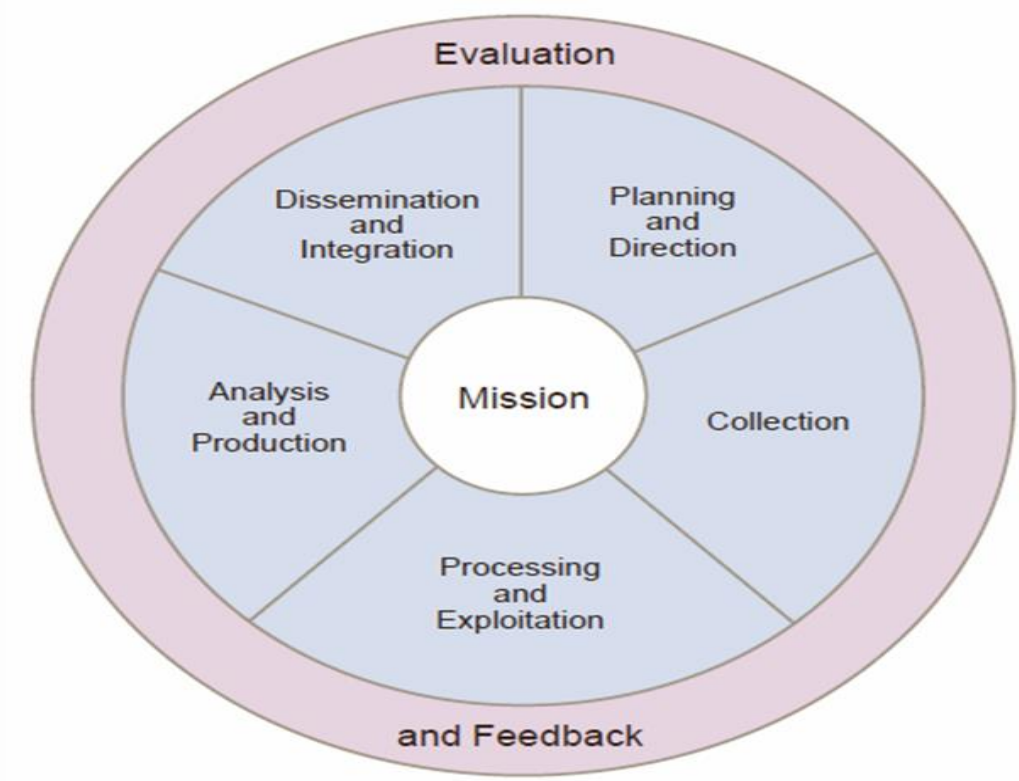
and offer opportunities for exploitation by decision-makers. Medical intelligence is not to be used, to take any advantage of medical vulnerabilities of any party as this would be a serious violation of fundamental ethical and legal conventions and likely have deleterious effects."[xix]

The UK defines MEDINT as 'Intelligence derived from medical, bio-scientific, epidemiological, environmental and other information related to human or animal health. This intelligence, being of a specific technical nature, requires medical expertise throughout its direction and processing within the intelligence cycle.[xx]

The model of the intelligence cycle describes in clear terms a way in which information necessary to inform public practices during health crises could be managed to meet the rapidly evolving needs of stakeholders working across the health security sector before, during, and after significant outbreaks.[xxi]

MEDINT is based on traditional intelligence methods and implies the application of the intelligence cycle in the field of medicine. It implies the collection and processing of data, assessment of data and predictions of all those risks. It involves information applied to the identification, characterization, and management of a risk, as applied to both medical and nonmedical countermeasures.

The objective of medical intelligence is to detect threats from infectious diseases, environmental hazards, biowarfare agents, and food and animal borne diseases. At the strategic level, the objective of medical intelligence is to identify broad trends in foreign military and civilian biomedical research and development that could present a threat to national security, such as life science technologies that can be used for either legitimate medical purposes or bioterrorism.



The intelligence cycle encompasses a number of domains:

Direction and planning

Management of the entire effort, from identifying the need for data to delivering an intelligence product to a consumer. It is the beginning and the end of the cycle--the beginning because it involves drawing up specific collection requirements, and the end because finished intelligence, which supports policy decisions, generates new requirements. Starting with direction, in which the intelligence requirements or questions to be answered are enumerated and gaps in current collection are recognized. The requirement appears, either from the decision makers or from the health intelligence service itself, which has found possible risks or threats that could affect it.[xxii]

The collection is the gathering of the raw information needed to produce finished intelligence. In preventing bioterrorism, intelligence collection or the gathering of the necessary data, plays an essential role. During health security crises, the government commits to clear directional requirements and enables cross-sector collection plans. There are many sources of information including:

Human Intelligence (HUMINT) is the collection of information from human sources.
The collection may be done openly, or it may be done through clandestine or covert means (espionage). HUMINT - resources can help identifying malicious actors who express interest in exploring bioweapons development and use.

Signals Intelligence (SIGINT) refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites. It involves the collection of communication data through interception of telephone conversations and emails and can survey internet metadata and location data. SIGINT is an intelligence technique that is less commonly used in infectious disease surveillance, but it may provide the best early warning system.

Imagery Intelligence (IMINT) is an intelligence gathering discipline which collects information by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar (SAR)—wherein the images are reproduced optically or electronically on film, electronic display devices, or other media.
Imagery intelligence provides detailed and precise information regarding the location and the physical characteristics of the threat and the environment in which it is operating. It is the primary source of information concerning key terrain features, installations, and infrastructure used to build detailed intelligence studies, reports, and target materials. Properly trained personnel, adequate time, and sophisticated equipment are needed to produce and provide IMINT.

Open-source intelligence (OSINT)- refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional

associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.), collection of publicly available information, could be a powerful source in early identification of emerging biothreats.

Processing and Exploitation involves converting the vast amount of information collected to a form usable by analysts. The transformation of the raw data might require decryption and decoding, translating the data, transforming the data for computer processing, storage and retrieval, adding background information to make the data more comprehensible, etc. One of the main challenges in the processing stage is the abundance of information, which makes differentiating between relevant and irrelevant information. This classification occurs within the processing stage.

The analysis is the conversion of basic information into finished intelligence. It includes integrating, evaluating, and analyzing all available data--which is often fragmentary and even contradictory--and preparing intelligence products .Analysts, who are subject-matter specialists, consider the information's reliability, validity, and relevance .They integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications of the information for the decision makers.

Dissemination is the phase of the intelligence cycle where the finalized intelligence product is provided to those who need it. [xxiii] Dissemination is the last step, which logically feeds into the first, is the distribution of the finished intelligence to the consumers, the same policymakers whose needs initiated the intelligence requirements.

The policymakers, the recipients of finished intelligence, then make decisions based on the information, and these decisions may lead to the levying of more requirements, thus triggering the Intelligence Cycle.

The intelligence cycle and MEDINT: The generation of medical intelligence products requires three important factors: highly qualified personnel in health referral intelligence methodology,

the existence of a timely and reliable quality information system, and technological support that performs advanced analysis processes.

Regular monitoring of information sources requires a highly trained epidemiology specialists with experience in handling information. The timely detection of threats and risks that may affect the health sector requires extraordinary sensitivity to be able to pertinently detect data and information that can become in a problem. The information gathered is assessed and analyzed by specialists against the core questions in order to produce actionable answers. Medical intelligence analysis can help assure that such potential biowarfare agents are not accidentally released or transferred to unlicensed facilities or hostile non-state actors. The analyst should have some sense of how well the intelligence requirements are being met and address any adjustments that need to be made. At the end of the process a public health report is generated that can be disseminated to all key stakeholders and decision makers, allowing for a cross-government strategic, operational and tactical response, with key decisions being taken by individuals in possession of an understanding of the wider pandemic impact. [xxiv]

The products of a medical intelligence system should help decision-makers to make the best decisions and to take medical countermeasures at an early stage to conserve the public health. A dialog between intelligence consumers and producers should occur before and continue after the intelligence has been received. Feedback assesses the degree to which the finished intelligence addresses the needs of the intelligence consumer and will determine if further collection and analysis is required. The connection between domestic and international processes for pandemic response necessitates information transfer not only within the nation states but between nation states and WHO under the requirements of the International Health Regulations (2005).

Conclusions

With the extraordinary disruption brought about by COVID-19, terrorist groups and other malicious actors may understand the catastrophic damage that can be caused by highly transmissible pathogens and other biological agents, and to use them in an attempt to deliberately cause the next pandemic.[xxv] The COVID-19 crisis has imposed the need for medical intelligence (MEDINT) to adapt to the new security reality.

We must take action now to safeguard the life sciences so society can reap all of their benefits, while guarding against the risks of exploitation and the potential for biotechnology catastrophe caused by terrorist groups or other powerful actors.

The full range of work to reduce biological risks posed by non-state actors includes prevention of bioweapons development and use, as well as early detection and effective response, so that biological events can be contained before they grow and spread out of control. The international nature of science, scientific publications and products, and possible security threats of bioterrorism require a common international approach to overseeing policies to deal with the threats. Biosecurity and Medical Intelligence have not been prioritized by the intelligence community in recent years and require a greater share of the resources committed to conventional warfare. [xxvi]

References

[i] INTERPOL- Bioterrorism incident pre-planning and response guide https://www.interpol.int/Crimes/Terrorism/Bioterrorism

[ii] "Testimony of Jaime M. Yassif, Ph.D., before the U.S. House Foreign Affairs Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation, hearing on 'Biosecurity for the Future: Strengthening Deterrence and Detection," via NTI website, December 8, 2021.

[iii] Patrick F. Walsh, Clemente, Jonathan. "Medical Intelligence," Intelligencer: Journal of U.S. Intelligence Studies 20, no. 2, (2013): 73-78.

[iv] Patrick F. Walsh, Intelligence, Biosecurity and Bioterrorism, Palgrave Macmillan, 2018.

[v] Spiers, E. (2010). *A History of Chemical and Biological Weapons*. London: Reaktion Books, pp - 102–125.

[vi] Koblentz, G. (2009). *Living Weapons*. New York: Cornell University Press, pp - 200–227.

[vii] Seth Carus, Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900. Washington, D.C., Center for Counterproliferation Research, National Defense University, 1998.

[viii] INTERPOL - Bioterrorism incident pre-planning and response guide https://www.interpol.int/Crimes/Terrorism/Bioterrorism

[ix] Vogel K.M., Ben Ouagrham-Gormley S. Anticipating emerging biotechnology threats: a case study *of CRISPR. Polit. Life Sci. 2018;37(2):203–219.*

[x] Gronvall, G. (2012). *Preparing for Bioterrorism*. Baltimore, MD: Center for Biosecurity of UPMC.

[xi] The NSABB dual-use research definition is available at *www.biosecurityboard.gov/faq.asp#14*.

[xii] Paul Cruickshank, Don Rassler, and Kristina Hummel, "A View from the CT Foxhole: Lawrence Kerr, Former Director, Office of Pandemics and Emerging Threats, Office of Global Affairs, U.S. Department of Health and Human Services," *CTC Sentinel* 15:4 (2022).

[xiii] Jamie Yassif, Preventing Catastrophic Bioterrorism: Guarding Against Exploitation of the Life Sciences and Biotechnology, CTCSENTINEL, at West Point, Volume15, Issue 5, May 2022. https://ctc.westpoint.edu/preventing-catastrophic-bioterrorism-guarding-against-exploitation-of-the-life-sciences-and-biotechnology/

[7] Ibid.

[xv] Hidemi Yuki, Lloyd Hough, Marc Sageman, Richard Danzig, Rui Kotani, and Terrance Leighton, "Aum Shinrikyo: Insights Into How Terrorists Develop Biological and Chemical Weapons," Center for a New American Security, July 20, 2011; Richard Danzig and Zachary Hosford, "Aum Shinrikyo – Second Edition – English," Center for a New American Security, December 20, 2012.

[xvi] Derrick Tin, Pardis Sabeti, Gregory R. Ciottone, Bioterrorism: An analysis of biological agents used in terrorist events, The American Journal of Emergency Medicine, Volume 54, April 2022, Pages 117-121. https://www.sciencedirect.com/science/article/pii/S0735675722000602

[xvii] Gemma Bowsher, Rose Bernard, Richard Sullivan, A Health Intelligence Framework for Pandemic Response: Lessons from the UK Experience of COVID-19, Health security, vol 18, no 6, December 14, 2020. https://www.liebertpub.com/doi/10.1089/HS.2020.0108

[xviii] https://www.militaryfactory.com/dictionary/military-terms-defined.php?term_id=3315

[xix] NATO's 2019 Allied Joint Doctrine for Medical Support (AJP-4.10)

[xx] Medical Support to Joint Operations, UK Ministry of Defense, January 2007, Joint Doctrine Publication 4-03 (JDP 4-03) 2nd Edition, p. 3-2

[xxi] Ostergard RL Jr. The West Africa Ebola outbreak (2014- 2016): a health intelligence failure? Intelligence Natl Secur. 2020;35(4):477-492.
[xxii] Phythian M, ed. Understanding the Intelligence Cycle. Abingdon, UK: Routledge; 2015.
[xxiii] Intelligence, n. 6c. OED Online. September 2020. Oxford University Press. Accessed September 15, 2020. https:// www-oed-com.proxy1.library.jhu.edu/view/Entry/97396
[xxiv] National Health Service (NHS). NHS Nightingale Hospital London. Accessed September 15, 2020. www.nightingalelondon.nhs.uk
[xxv] "Testimony of Jaime M. Yassif, Ph.D., before the U.S. House Foreign Affairs Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation, hearing on 'Biosecurity for the Future: Strengthening Deterrence and Detection," via NTI website, December 8, 2021.
[xxvi] Jamie Yassif, Preventing Catastrophic Bioterrorism: Guarding Against Exploitation of the Life Sciences and Biotechnology, CTCSENTINEL, at West Point, Volume15, Issue 5, May 2022. https://ctc.westpoint.edu/preventing-catastrophic-bioterrorism-guarding-against-exploitation-of-the-life-sciences-and-biotechnology/